Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Currently amended) A method for providing a user device with a set of access codes, the method comprising:

~~in the user device, storing an encryption key and an identification code, and sending a message containing the identification code to a server via a communications network;~~

~~in the server,~~

receiving from a user device a first message comprising an identification code associated with an encryption key stored in the user device, wherein the first message is sent via a communications network;

storing an encryption key corresponding to the encryption key and the identification code stored in the user device,

allocating the set of access codes on receipt of the identification code from the user device,

performing a look up function based on the identification code received in the message to retrieve the encryption key from storage,

encrypting the set of access codes using the retrieved encryption key to produce an encrypted set, ~~and~~

sending a second message containing the encrypted set to the user device for storing ~~via the network;~~

~~in the user device, decrypting the encrypted set received from the server using the key in storage, and storing the decrypted set of access codes for use by a user of the user device;~~ and,

upon ~~the~~ a number of unused access codes for the user device reaching a predetermined threshold, ~~in the server,~~ sending a third message containing a new set of access codes to the user device via the network, wherein the new set of access codes are encrypted with the encryption key associated with the identification code~~;~~

~~in the user device, storing the new set for use by a user of the user device; and~~

~~selectively:~~

~~in the user device, tracking the access codes used by the user, generating a request in~~

~~response to the number of unused access codes reaching a predetermined threshold, and sending a~~

~~message containing the request to the server; and~~

~~in the server, sending the message containing the new set of access codes on receipt of the~~

~~request; or~~

~~in the server, tracking the access codes used by the user, and sending the message containing the new set of access codes to the user device in response to the number of unused access codes reaching a predetermined threshold; or~~

~~in the server, generating a new key, encrypting the new key with the previous key, and sending a message containing the encrypted new key to the user device via the network; and, in the user device, decrypting the new key received from the server using the previous key, and storing the decrypted new key in place of the previous key; or~~

~~in the server, encrypting a new set of access codes with the new key to produce a new key encrypted set, and sending a message containing the new key encrypted set to the user device via the network, and,~~
~~in the user device, decrypting the new key encrypted set using the new key, and storing the decrypted new set for use by a user of the user device; or~~

~~in the user device, generating a public/private key pair, and sending a message containing the public key of the pair to the server via the network,~~
~~in the server, generating a session key, encrypting the set of access codes with the session key to produce a session key encrypted set, encrypting the session key with the public key to produce an encrypted session key, sending a message containing the session key encrypted set and the encrypted session key to the user device via, the network, and,~~
~~in the user device, decrypting the encrypted session key with the private key of the pair to recover the session key, decrypting the session key encrypted set with the recovered session key to recover the set, and storing the decrypted set for use by a user of the user device.~~

2.-41. (Canceled)

42. (New) The method of claim 1 further comprising:

receiving a request for the new set of access codes from the user device, wherein the user device tracks its own access code use, comparing the number of unused access codes to the predetermined threshold after every use; and

sending the new set of access codes to the user device upon receipt of the request.

43. (New) The method of claim 1 further comprising:

tracking the access codes used by the user device, and

sending the new set of access codes to the user device in response to the number of unused access codes reaching a predetermined threshold.

44. (New) The method of claim 42 wherein the request is sent from the user device responsive to a manual input from the user.

45. (New) The method of claim 1 further comprising:

receiving from the user device a fourth message comprising a public key of a public/private key pair generated at the user device;

generating a session key;

encrypting the set of access codes with the session key to produce a session key encrypted set;

encrypting the session key with the public key to produce an encrypted session key; and

sending a message containing the session key encrypted set and the encrypted session key to the user device via the network.